

Response under 37 C.F.R. 1.111
Serial No. 09/672,206
Page 5 of 16

Amendments to the Claims

Please amend the claims as follows:

1. (Currently Amended) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server S disposed in a network of interconnected elements communicating using the TCP protocol, comprising the steps of

controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor,

establishing a first TCP connection between one or more clients originating said packets and said web guard processor, and a second TCP connection between said web guard processor and said server, so that packets can be transmitted between said one or more clients and said server,

monitoring the number of timed-out connections between said web guard ~~server processor~~ and said one or more clients,

if the number of timed-out connections between said web guard ~~server processor~~ and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor.

2. (Currently Amended) The method of claim 1 ~~wherein said process further includes~~ further comprising the step of generating an alarm indicating that said server is likely to be under attack.

3. (Currently Amended) The method of claim 1 including the further steps of determining if the number of timed-out connections between said web guard ~~server processor~~ and said clients exceeds a second predetermined threshold, and if so, controlling said switch to delete all SYN packets destined for said server.

Response under 37 C.F.R. 1.111
Serial No. 09/672,206
Page 6 of 16

4. (Currently Amended) The method of claim 3 ~~wherein said process further includes further comprising the step of~~ generating an alarm indicating that said server is under attack.
5. (Original) The method of claim 1 further including the step of notifying said server that it is under attack.
- A4
6. (Original) The method of claim 1 further including the step of notifying other web guard processors in said network that said server is under attack.
7. (Original) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server S disposed in a network of interconnected elements communicating using the TCP protocol, said attack originating from a malicious host generating SYN packets destined for said server, said method comprising the steps of
- arranging a switch receiving said SYN packets destined to said server to forward said SYN packets to a TCP proxy arranged to operate without an associated cache,
 - whereby said TCP proxy, when subject to a CSDoS attack, does not successfully establish a TCP connection with said malicious host, and no TCP connection is made from said TCP proxy to said server, thereby protecting said server from said attack.
8. (Currently Amended) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server S disposed in a network of interconnected elements communicating using the TCP protocol, comprising the steps of
- forwarding a statistical sampling of said packets from a switch in said network to a processor,

Response under 37 C.F.R. 1.111
Serial No. 09/672,206
Page 7 of 16

A4

If packets in said sampling indicate an attack, altering the operation of said switch to reduce the effects of said attack.

9. (Original) The method of claim 8 wherein said switch is arranged to discard packets in the event an attack is detected.